BY ORDER OF THE COMMANDER,
16TH SPECIAL OPERATIONS WING (AFSOC)

HURLBURT FIELD INSTRUCTION 10-1101

15 OCTOBER 1999

OPERATIONS

OPERATIONS SECURITY (OPSEC) INSTRUCTIONS, 16TH SPECIAL OPERATIONS WING

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally via the Electronic Transaction System (ETS) site at: http://afpubs.hq.af.mil. If you lack access, contact the OPR and/or publications manager.

OPR: 16 SOW/XPF (TSgt Michael Cotton)

Certified by: 16 SOW/XP (Lt Col Brian Johnson)
Pages: 32
Distribution: F

This publication implements Air Force Policy Directive (AFPD) 10-11, Air Force Instruction 10-1101, *Operations Security*, USSOCOM Directive 530-1, *Operations Security*, Air Force Special Operations Command (AFSOC) Instruction 10-1101, *Operations Security (OPSEC) Instructions*; DoD Directive 5205.2, *DoD Operations Security Program*; Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3210.01, *Joint Information Warfare Policy*; CJCSI 3213.01, *Joint Operations Security*; and all Operations Security requirements for DoD Instruction 5000.2, *Defense Acquisition Management Policies and Procedures*. OPSEC is one of the critical pillars in C2W strategy, it also directly supports AFPD 10-7, *Command and Control Warfare (C2W)*. It seeks to provide guidance for 16th Special Operations Wing (SOW) unit OPSEC managers. Though each unit and their mission is unique, these basic principles can be universally applied.

Chapter 1

INTRODUCTION

1.1. Definition. OPSEC is a process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to a.) identify those actions that can be observed by potential adversaries; b.) determine indicators that could be interpreted or pieced together to derive critical information in time to be useful to an adversary; and, c.) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC should be closely coordinated with security disciplines (HFI 31-101, *Physical Security*; AFI 31-401, *Information Security*; and AFPD 33-2, *Information Protection*) to ensure that all aspects of sensitive activities are protected. Potential exploitation of open sources and observable actions are a primary focus of OPSEC analysis. These sources are generally unclassified and, consequently, more difficult to control. The analysis facilitates risk management by providing decision-makers with a means of directly assessing how much risk they are willing to accept.

1.2. Air Force Operations Security. The Air Force implements the OPSEC process in all functional areas. Commanders are responsible for all OPSEC awareness throughout their organizations and for integrating the OPSEC process throughout appropriate mission areas.

1.2.1. OPSEC is an integrated component of Information Warfare (IW). It provides a means of detecting and controlling an adversary's actions on our military information functions. OPSEC assists in protecting IW capabilities and intentions from adversary knowledge and attack.

1.2.2. Organizations that fail to implement OPSEC are more likely to unintentionally give away critical information and expose missions to increased risk.

1.2.3. OPSEC should be considered simultaneously with complementing and competing activities to obtain maximum effectiveness. Planners and decision-makers should consider operational objectives, strategies, deception, psychological operations, electronic warfare, and traditional security measures as a single effort to control perceptions, decisions, Public Affairs and activities of an adversary.

1.2.3.1. Complementing Activities. There are a host of other concepts, activities, procedures, disciplines, and systems that complement the positive control of information. When they are considered with OPSEC measures as alternative methods for controlling information, flexibility and ultimately, greater security is added to operations. When OPSEC measures are planned in conjunction with deception, psychological operations, electronic combat and other traditional security programs, synergism occurs in the C2W environment.

1.2.3.2. Competing Activities. Several factors exist that continually compete with information protection. Examples include: information releases to the media, foreign military sales, treaty provisions, business agreements, and normal operating procedures.

Chapter 2

THE OPERATIONS SECURITY PROCESS

2.1. General. OPSEC analysis is accomplished through the use of a five-step **process**. This **process** is the most important aspect of OPSEC. It determines how well OPSEC is being integrated into both mission planning and execution. Each application of the process represents a closed loop effort that is to be reapplied as activities, events, situations and operations change. NOTE: The same process used to plan an operation is also the one used to survey or, evaluate it. In fact the process can be applied to any situation in which there is competition. The five steps of the OPSEC process are:

2.1.1. Identification of Critical information (and its indicators).

2.1.2. Analysis of Threats.

2.1.3. Analysis of Vulnerabilities.

2.1.4. Assessment of Risk.

2.1.5. Application of Appropriate Countermeasures.

2.1.6. OPSEC will be applied to the following five areas, plus other activities as deemed appropriate. A flow description of each is at **Attachment 8**-10:

2.1.6.1. Training exercises

2.1.6.2. Current Operations to include SORTS/Deployment reporting

2.1.6.3. Contingency Operations/Planning

2.1.6.4. Force and doctrine development, and defense acquisition system process

2.1.6.5. Resource programming/allocation process

2.2. Identification of Critical information. Those individuals responsible for the development and execution of the operation are best situated to identify critical information. They possess the intimate familiarity necessary to properly apply the OPSEC concept to the task at hand. The 16 SOW standing Critical Information List is **Attachment 5**.

2.2.1. Mission critical information will be developed and appropriately revised to reflect changing situations. Critical information is usually only critical for a prescribed period of time. The need to control or protect specific items of information will most likely change as an operation progresses and/or as the adversarial threat changes.

2.2.2. Directors and units will identify contractor requirements to control and protect certain critical information. Contractors will continue to control such information until notified, in writing, that the need for OPSEC measures no longer exists.

2.3. Threat Analysis. OPSEC planners and commanders must use current threat information to develop appropriate OPSEC measures. This information is available from authorized USAF and DoD intelligence and counterintelligence organizations. An OPSEC threat analysis includes identifying adversaries and their capabilities, limitations, and intentions to collect, analyze and use critical information and OPSEC indicators against friendly forces. This analysis must be tailored to the particular operation, test, project, geographic region or facility.

2.3.1. The Air Force Office of Special Investigations (AFOSI) produces counterintelligence studies and analyzes multi-discipline intelligence threats posed to US Air Force and DoD programs and resources by Foreign Intelligence services. Contact Detachment 309 at Hurlburt Field.

2.3.2. To request Foreign Intelligence threat information, call the Air Force Information Warfare Center's Operations Support Central (AFIWC/OSC) at DSN 969-2191/2152 for 24-hour support.

2.4. Vulnerability Analysis. Two conditions must be present for an OPSEC vulnerability to exist: (1) There is a weakness that could reveal critical information and (2) there is an adversary with both the intent and capability to exploit that weakness (i.e., a threat). Efforts must be taken to identify an organization's potential vulnerabilities. Once identified, these vulnerabilities must be either outright denied or proactively controlled.

2.4.1. At times, it may not be cost-effective or even possible to alter the source of an OPSEC indicator. In that instance, it may be prudent to take a proactive approach by attempting to disrupt or confuse the adversary's ability to collect and/or properly interpret the information. Hence, OPSEC measures should also be considered as a means to control the adversary and their ultimate comprehension or use of the information when an OPSEC indicator can not be modified.

2.5. Risk Assessment. Risk assessment involves informed estimates of an adversary's capability to exploit a friendly weakness; the potential effects such exploitation will have on an operation, activity or weapon system and a cost-benefit analysis of actions contemplated to counter the vulnerability. Risks are reduced or eliminated by employing OPSEC measures to control the availability of information to the adversary.

2.5.1. OPSEC Program Managers, in concert with other planners and with the assistance of intelligence and counterintelligence organizations, will accomplish risk assessments and provide recommendations to commanders (the senior decision-makers). Commanders, who are ultimately responsible for mission success, must decide whether or not to employ OPSEC measures.

2.6. OPSEC Measures. OPSEC measures are employed to counter or eliminate vulnerabilities that point to or divulge critical information. They help to deny critical information by controlling the raw data adversaries use to make decisions, thereby limiting their effectiveness and possibly even their credibility. OPSEC measures also enhance friendly capabilities by increasing the potential for surprise and effectiveness of friendly military forces and weapon systems.

2.6.1. OPSEC measures can be used to eliminate the source of indicators or vulnerabilities of friendly actions to exploitation by adversary intelligence systems through action control. Specifically, select what actions to take; decide whether or not to execute actions necessary to accomplish tasks. When it is impossible or impractical to use action control procedures, countermeasures may be employed to disrupt effective adversary information gathering or prevent their recognition of indicators when collected materials are processed. Use unit system designs and procedures to create diversions, camouflage, conceal, jam, or use force against adversary information gathering and processing capabilities. Another method is to employ counter-analysis. The objective of counter-analysis is to prevent accurate interpretation of indicators during adversary analysis of collected materials. Confuse the adversary analyst through deception techniques such as covers. Finally, protective measures are methods to create closed information systems to prevent adversaries from gaining access to information and resources. Examples include cryptologic systems and standardized security procedures.

2.6.2. At the very heart of the OPSEC concept is risk management by commanders and senior decision-makers. OPSEC measures must preserve the effectiveness of friendly military capabilities while controlling the adversarial exploitation of critical information to the maximum extent possible. Determining the delicate balance between OPSEC measures and operational needs is always the commander's decision. Commanders must decide whether organizational activities that yield OPSEC indicators jeopardize the attainment of friendly initiative, surprise or superiority and if so, to what degree?

2.6.3. OPSEC measures that control critical information and OPSEC indicators must be developed as operations are planned to complement mission objectives and strategies. Individuals who are most familiar with the operation should develop and recommend OPSEC measures. However, an office of primary responsibility within the plans division should centrally supervise OPSEC measures and/or operations structure to ensure their purpose is consistent with mission needs.

2.6.4. 16 SOW and supporting units will develop and execute OPSEC measures that:

2.6.4.1. Are consistent with operational mission needs

2.6.4.2. Deny (by controlling) critical information, OPSEC indicators, and the sources of such information to prevent degrading the effectiveness of friendly plans, forces, weapon systems, defense systems, and command and control

2.6.4.3. Degrade the effectiveness of adversary decisions, command and control, and weapon systems to limit the effectiveness of adversary forces

2.6.5. OPSEC Planning/Writing Basic OPSEC Plans. Ref. AFSOCI 10-1101, pg. 07, par. 2.8

Chapter 3

16 SOW OPERATIONS SECURITY PROGRAM

3.1. Purpose. To provide 16 SOW decision-makers at all levels with a means of promoting understanding and awareness in the integration and application of OPSEC. The 16 SOW OPSEC Program provides the wing and all subordinate units with standardized policy to facilitate an effective OPSEC program.

3.2. 16 SOW Operations Security. The 16 SOW implements the OPSEC process in all functional areas. The goal is to develop and maintain a standing program that will prevent an adversary's timely exploitation of critical friendly information. This goal supports HQ AFSOC's number one command goal, to "enhance combat readiness" through improved survivability. In order to achieve this goal, we must:

3.2.1. Develop an effective plan that integrates the OPSEC process across the entire spectrum of 16 SOW's daily activity and applies the analysis process when critical information is identified.

3.2.2. Continually assess current operations, OPLAN/CONPLAN preparations, training activities, force development plans and programs, Mission Area Plans (MAPs), and Weapon System Roadmaps.

3.2.3. Incorporate traditional security disciplines and staff functions as integral players in OPSEC planning and execution.

3.2.4. Integrate OPSEC into the wing's Information Operations/Warfare program.

3.2.5. Conduct an aggressive OPSEC training program.

3.3. Commander Involvement. Commanders are responsible for the appropriate use of the OPSEC concept and must ensure OPSEC guidance is developed as early as possible in the planning and coordination process. Commanders may delegate authority for the management of the OPSEC program and the execution of OPSEC measures, but must personally make the key decisions with respect to the implementation of OPSEC measures and provide necessary guidance to subordinates.

3.4. Organization. The 16 SOW Commander will appoint a program manager for the wing to administer the overall OPSEC program. Each Group/Squadron Commander will appoint an OPSEC Point of Contact (POC) who will coordinate OPSEC matters in their organization. Unit POC's are responsible to the 16 SOW program manager. OPSEC Program Managers must be familiar with higher echelon direction, goals, objectives, strategies, activities and the personnel who participate in those activities to understand what information is critical and how it applies to the organization's primary mission. The OPSEC program manager can then be invaluable when helping to develop and recommend OPSEC measures that will have a realistic and positive effect on the outcome of the mission. Unit OPSEC Program Managers or their designated alternate will attend 16 SOW OPSEC working groups and meetings.

3.5. Training and Education. The purpose of OPSEC training and education is to ensure everyone in the wing understands: a) the positive benefits of OPSEC; b) the effects of Foreign Intelligence collection on mission effectiveness and c) what AFSOC does to control the exploitation of critical information. OPSEC education and training should be continuing and ongoing throughout each Service member, civilian employee and, government contractor's period of service in the wing.

3.5.1. Training activities from the Joint Readiness Exercise (JRX) down through the small unit tactics level should contain OPSEC considerations and applications appropriate to training goals where tasks, conditions and standards are applied. Real-world sensitivities relating to capabilities and methodologies to which training activities are focused may also require the application of OPSEC protective measures.

3.5.2. OPSEC considerations will be included in the evaluation of units on training tests, readiness inspection and field exercises.

3.5.3. Unit OPSEC Training. The purpose of unit OPSEC training is to ensure all wing personnel understand the Foreign Intelligence threat as it relates to their mission; critical information for the missions they support; job specific OPSEC indicators; and the OPSEC measures they will execute. Initial training will be developed and presented to newly assigned personnel within 90 days after arrival for duty. As a minimum, it must include:

3.5.3.1. Duty related mission critical information and OPSEC indicators

3.5.3.2. Foreign Intelligence threat to missions supported and conducted

3.5.3.3. Individual responsibilities

3.5.4. Annual Training. Once per year every AFSOC individual must receive OPSEC training which covers the items in **Attachment 6**. OPSEC Program Managers and POC's are responsible for annual training of their personnel. To assist in providing a standardized product where applicable, the HQ AFSOC OPSEC program manager will provide training materials to the trainers. The decision to use the AFSOC training material rests with the OPSEC instructor, however all categories shown at **Attachment 6** must be covered.

3.5.5. OPSEC Program Managers will interface with supported and supporting units and offices to ensure continuity of effort and complementary OPSEC measures.

3.6. Evaluations. There are several methods used to evaluate OPSEC programs and the effectiveness of OPSEC measures:

3.6.1. OPSEC Surveys. OPSEC surveys help determine how well an organization's Critical Information is being denied to adversaries. Guidance for conducting OPSEC surveys can be found in AFMAN 10-1106, AIA/OSW OPERATIONS SECURITY ASSESSMENT HANDBOOK, and JCS PUB 3-54.

3.6.2. Telecommunications Monitoring. The express purpose of telecommunications monitoring is to provide feedback to the commander's OPSEC program. Telecommunications monitoring involves the electronic monitoring and analysis of unsecured phones, faxes, radios, and computers to estimate an organization's OPSEC posture. Telecommunications monitoring can be coordinated through the wing OPSEC program manager.

3.6.3. OPSEC Appraisals and Status Reports. OPSEC Program Managers and directorate POC's will accomplish an annual appraisal through the use of the self-inspection checklist at **Attachment 7**. Unit program managers will submit a report IAW **Attachment 8** to 16 SOW OPSEC program manager NLT 1 Oct annually.

3.6.4. Inspector General Evaluations. The extent to which Air Force components maintain their OPSEC programs will be a key area for evaluation during visits by inspectors general IAW AFI

90-201, A4.2.3., *Inspector General Activities*, concerning “common core criteria”. Areas of interest will include: commander’s involvement, the integration of the OPSEC concept into unit plans and operating procedures, MAPs and Weapon System Roadmaps, training, funding, program placement, intelligence support and counterintelligence support to the OPSEC program (A4.2.3. Inspected Areas, Security: “Were OPSEC procedures incorporated into plans and followed throughout the exercise?”).

DAVID J. SCOTT, Colonel, USAF
Commander

Attachment 1

TERMS AND DEFINITIONS

A1.1. Capability. The ability to execute a specified course of action. (A capability may or may not be accompanied by an intention) (Joint Pub 1-02). NOTE**:** When considering vulnerabilities, a capability requires the physical and mental attributes and sufficient time required for performance.

A1.2. Closed Information Systems. A group of interacting or interdependent procedures and devices acting together to provide information to its users and totally prohibit access to outsiders. It provides its users strict secrecy, prevents information compromise and completely protects the integrity and availability of the information within the system. Examples are secured telephone systems, isolated computer stations, and activities within a building that cannot be detected or observed from the outside.

A1.3. Critical Information. Specific facts about friendly intentions, capabilities, limitations, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

A1.4. Information Operation/Warfare . The integrated use of Operations Security (OPSEC), Military Deception, Psychological Operations (PSYOP), Electronic Warfare (EW), and Physical Destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary command and control capabilities against such actions. Information Operations/Warfare applies across the operational continuum and all levels of conflict.

A1.5. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs. (Executive Order 12333)

A1.6. Exploitation. 1. Taking full advantage of success in battle and following up initial gains. 2. Taking full advantage of any information that has come to hand for tactical or strategic purposes. 3. An offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth. (Joint Pub 1-02)

A1.7. Foreign Intelligence. Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence (except for information on international terrorist activities).

A1.8. Intelligence Systems . Any formal or informal system to manage data gathering, to obtain and process the data, to interpret the data, and to provide reasoned judgments to decision makers as a basis for action. The term is not limited to intelligence organizations or services but includes any system, in all its parts, that accomplishes the listed tasks. (Joint Pub 1-02)

A1.9. Intention . An aim or design (as distinct from capability) to execute a specified course of action. (Joint Pub 1-02)

A1.10. Military Deception. Actions executed to mislead foreign decision-makers, causing them to derive and accept desired appreciation of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives. There are three categories of military deception: strategic, tactical, and Department/Service (see Joint Pub 1-02)

A1.11. Multidiscipline Counterintelligence (MDCI) Threat Assessment. All–source (HUMINT, SIGNET, and IMINT) analysis of threats to a specific activity, location, operation, project, weapons or other system, deployment, or exercise.

A1.12. Open Information Systems . Any information system or activity which may be accessed or observed by personnel outside of the system and provides information by open sources or OPSEC indicators. Open information systems use open source information or provide OPSEC indicators that may be observed by adversaries and adversarial weapon systems. Examples are non-secure telephone systems, computer systems connected to outside lines, and non-secure radio systems.

A1.13. OPSEC Appraisal. An internal evaluation or assessment of the OPSEC program, usually by the OPSEC program manager, to determine the vitality and credibility of his own program. For example: Are the components of the program in place? Have critical information and OPSEC indicators been identified and coordinated? Are necessary personnel apprised of intelligence collection methods?; etc.

A1.14. OPSEC Indicator. Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (Joint Pub 1-02)

A1.15. OPSEC Measure. Methods and means to reduce or eliminate OPSEC vulnerabilities by controlling both Critical information and the OPSEC indicators of that critical information. The following categories apply:

A1.15.1. Action Control. Methods to eliminate or prevent detection of OPSEC indicators. Example: Adjusting schedules and activities and delaying information releases. First, plan activities necessary to conduct and support an operation; then, control the conduct (timing, place, etc.) of those activities to eliminate or substantially reduce OPSEC indicators.

A1.15.2. Countermeasures. Methods to disrupt adversary information gathering sensors and data links, or preventing an adversary from obtaining, detecting, or recognizing OPSEC indicators. Examples are jamming, interference, diversions, and force. The objective is to disrupt effective adversary information gathering, processing, analysis, and distribution. Use units, system designs, and procedures to create diversions, camouflage, concealment, jamming, threats, police powers, and force against adversary information gathering, processing, and distribution capabilities.

A1.15.3. Counteranalysis . Methods to affect the observation and/or interpretation of adversary intelligence analysts. Examples are military deceptions and covers. The objective is to prevent accurate interpretations of OPSEC indicators during adversary data analysis. Confusing the adversary analyst through deception techniques does this.

A1.15.4. Protective Measures . Methods to create closed information systems to prevent adversaries from gaining access to information and resources. Examples include cryptologic systems and standardized security procedures.

A1.16. OPSEC Survey. The formal evaluation of a function, operation, activity, facility, project, or program designed to identify OPSEC vulnerabilities and provide recommendations to reduce or eliminate them. The establishment of a dedicated survey team characterizes OPSEC surveys, use of the OPSEC process, the analysis of all sources of information, the use of a multidiscipline approach and an adversarial viewpoint to assess the effectiveness of OPSEC measures, and the preparation of a formal report.

A1.17. OPSEC Vulnerability. A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. (Joint Pub 1-02)

A1.18. Psychological Operations (PSYOP). Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (Joint Pub 1-02)

A1.19. Vulnerability. 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (Joint Pub 1-02) Weapon System. A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. (Joint Pub I02)

A1.20. Weapon System. A combination of one or more weapons with all related equipment, materials, services, personnel and means of delivery and deployment (if applicable) required for self-sufficiency. (Joint Pub 1-02)

Attachment 2

ACRONYMS

AETC	Air Education and Training Command
AFIWC	Air Force Information Warfare Center
AFOSI	Air Force Office of Special Investigations
AFSOC	Air Force Special Operations Command
AIA	Air Intelligence Agency
C2W	Command and Control Warfare
C3	Command, Control and Communications
CISO	Counter Intelligence Staff Officer
CM	Countermeasure
COMAFSOC	Commander, AFSOC
COMSEC	Communications Security
CONOPS	Concept of Operations
CONPLAN	Concept Plan
DO	Director of Operations
EW	Electronic Warfare
EXPLAN	Execution Plan
FLTS	Flight Test Squadron
FRAGORD	Fragmentation Order
HHQ	Higher Headquarters
HUMINT	Human Intelligence
IAW	In Accordance With
IMINT	Imagery Intelligence
IS	Intelligence Squadron
IW	Information Warfare
JCS	Joint Chiefs of Staff
MAP	Mission Area Plan
MDCI	Multidiscipline Counter Intelligence
MNS	Mission Need Statement
OPCON	Operational Control
OPLAN	Operation Plan

OPORD	Operation Order
OPSEC	Operations Security
ORD	Operational Requirements Document
POC	Point of Contact
PSYOP	Psychological Operations
SIGINT	Signals Intelligence
SOG	Special Operations Group
SOP	Standard Operating Procedures
SOW	Special Operations Wing
STG	Special Tactics Group
TD	Tactical Deception
USAFSOS	United States Air Force Special Operations School
USCINCSOC	Commander-In-Chief, United States Special Operations Command
USSOCOM	United States Special Operations Command

Attachment 3

HIGHER HEADQUARTERS AND SUPPORTING COMMAND RESPONSIBILITIES AND AUTHORITIES

A3.1. Headquarters United States Air Force (HQ USAF) responsibilities (from AFI 10-1101). The Deputy Chief of Staff for Plans and Operations (HQ USAF/XO) is the office of primary responsibility for the Air Force OPSEC program.

A3.1.1. HQ USAF/XO , through the Technical Plans Division (HQ USAF/XOOP), will:

A3.1.1.1. Develop OPSEC doctrine, policies, plans, and procedures consistent with joint and DoD OPSEC guidance.

A3.1.1.2. Designate an overall Air Force OPSEC program manager.

A3.1.1.3. Provide to J-3, Joint Staff, Attn: J-33/STOD/TSB, copies of all current Service OPSEC program directives and/or policy implementation documents.

A3.1.1.4. Support the National and DoD OPSEC programs as necessary.

A3.1.1.5. Provide management and annual review of the Air Force OPSEC program.

A3.1.1.6. Recommend to the Deputy Under Secretary of Defense (Policy) for Policy Support changes to policies, procedures and practices of DoD OPSEC program.

A3.1.1.7. Utilize OPSEC training, advice, and services provided by the National Security Agency (NSA) and the Interagency OPSEC Support Staff (IOSS) when appropriate.

A3.1.2. HQ USAF/IN will, upon request from the commander concerned, provide Air Force units and supporting organizations with current and mission specific Foreign Intelligence threat information. Threat information will identify current and potential adversaries and include Foreign Intelligence capabilities, intentions, resources, doctrine and state-of-the-art collection methods.

A3.1.3. HQ AFOSI will, upon request from the commander concerned, provide Air Force units with current mission specific counter intelligence and MDCI threat assessment information.

A3.2. HQ USSOCOM Responsibilities (from USSOCOM D 530-1). Organize, budget, and staff to meet the OPSEC requirements of CJCS MOP 29 and objectives in this publication. As a minimum, an OPSEC Steering Committee and a Command OPSEC officer will be identified with the following listed duties and responsibilities:

A3.2.1. HQ USSOCOM SOJ3 will:

A3.2.1.1. Exercise primary staff responsibility for the USSOCOM OPSEC program.

A3.2.1.2. Provide for the integration of OPSEC into the curriculum/objectives of education/training activities.

A3.2.1.3. Chair the USSOCOM OPSEC committee.

A3.2.2. HQ USSOCOM Steering Committee will:

A3.2.2.1. Meet quarterly or at the direction of the chairman to steer the USSOCOM OPSEC program.

A3.2.2.2. Recommend USSOCOM OPSEC policy.

A3.2.2.3. Nominate ongoing headquarters activities and operations for OPSEC surveys.

A3.2.2.4. Monitor OPSEC effectiveness of HQ USSOCOM, subordinate commands and contractual activities.

A3.2.2.5. Direct OPSEC awareness training as may be required.

A3.2.2.6. Assist with training of directorate OPSEC action officers to ensure support goals and objectives outlined in this publication.

A3.2.2.7. Integrate staff functions and traditional security programs into a mutually supporting relationship with the USSOCOM OPSEC program.

A3.2.3. HQ USSOCOM Command OPSEC Officer will:

A3.2.3.1. Maintain liaison with other agencies, activities, and commands for the purposes of coordination, training information, and operational support.

A3.2.3.2. Represent USCINCSOC at OPSEC meetings and conferences.

A3.2.3.3. Administer the functions of the OPSEC Committee as directed by the operations Director, J3.

A3.2.3.4. Conduct the command OPSEC review program consisting of; an annual OPSEC Conference, necessary actions relative to submissions of component commands annual OPSEC report, and annual command visits to component commands and other selected activities to ensure coordination of OPSEC actions and issues.

A3.2.3.5. Submit annual OPSEC program reports as required by CJCS MOP 29.

A3.2.3.6. Assist accomplishment of surveys and assessments

A3.2.3.7. Assist with acquisition of special technical support for assessments and surveys as may be required by HQ USSOCOM and component commands.

A3.2.3.8. Store and maintain command OPSEC-related information.

A3.2.4. HQ USSOCOM Counter Intelligence Staff Officer (CISO) will coordinate counter intelligence requirements with the J3, establish liaison with the command OPSEC officer and ensure that a mechanism for passage of information on the adversary intelligence collection and sabotage capabilities is established. The CISO will assist the Operations Directorate in the conduct of OPSEC vulnerability assessments and surveys and assist component command CI activities as may be required.

A3.2.5. HQ USSOCOM Inspector General will conduct an independent evaluation of the OPSEC program on an annual basis, reporting the results to Commander in Chief; copy to SOJ3.

A3.3. Air Intelligence Agency/Air Force Information Warfare Center Responsi bilities Air Intelligence Agency (AIA), with the resources of Air Force Information Warfare Center (AFIWC), is tasked to provide administrative support, technical services, and assistance as required to HQ USAF/XOOS for OPSEC program development, planning, and execution. The focal point for OPSEC support and expertise within AFIWC is the Operations Support Directorate (OSW). Direct communication is authorized between OSW and the MAJCOM OPSEC program managers. Informal communication is authorized between OSWand their other Service and DoD agency counterparts for the exchange of information on OPSEC program matters. AIA/AFIWC will develop and maintain:

A3.3.1. The capability to accomplish thorough, professional level, OPSEC surveys.

A3.3.2. OPSEC training aids and materials to support both an active marketing plan and a MAJCOM training program to be presented by OPSEC program managers in the field

A3.3.3. A recurring, in-depth training course for OPSEC program managers and other personnel who perform OPSEC surveys.

A3.3.4. AIA/AFIWC will also make available to all Air Force units and supporting organizations current mission specific, Foreign Intelligence threat information. Threat information will identify current and potential adversaries and include Foreign Intelligence capabilities, intentions, resources, doctrine and state-of-the-art intelligence collection methods.

A3.3.5. Foreign Intelligence . AIA is responsible for providing Foreign Intelligence threat information in support of the Air Force OPSEC program. Such data includes information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counter intelligence (except for information on international terrorist activities).

A3.4. Air Force Office of Special Investigations (AFOSI). AFOSI is the USAF agency responsible for counter intelligence and MDCI threat assessments. They produce studies, estimates, and analysis in support of the OPSEC program. Such data includes information relating to the capabilities, intentions, resources, doctrine, and collection methods of Foreign Intelligence services or international terrorist activities. In addition, AFOSI will support OPSEC program managers and commanders with OPSEC survey support, planning, and training assistance, and a complete range of studies, reports, and analytical products. OSI Detachment commanders will assist their local commanders with access, as necessary, to threat information from sources outside the Air Force.

A3.5. Air Education and Training Command (AETC) . AETC will provide for a basic, but thorough, introduction of OPSEC to all new military Air Force members. The block of training must include:

A3.5.1. The purpose and value of the OPSEC concept.

A3.5.2. An overview of the process.

A3.5.3. An introduction to the application of OPSEC measures.

A3.5.3.1. OPSEC will be presented as this is the way we do our day-to-day business in the United States Air Force. AETC will also provide general OPSEC education, as appropriate, in all professional level courses. Professional level materials should include the purpose and use of the OPSEC concept, the process, complementing and conflicting concepts, OPSEC planning, and command responsibilities.

Attachment 4

16 SOW, UNIT, AND INDIVIDUAL RESPONSIBILITES

A4.1. Commander Responsibilities. Though the OPSEC program helps commanders to make and implement decisions, the decisions themselves are the commander's responsibility. Commanders must understand the risk to the mission and then determine whether OPSEC measures if any, are required. Commanders must make the decisions that risk mission effectiveness.

A4.1.1. Commanders at every level will:

A4.1.1.1. Be responsible for their OPSEC program.

A4.1.1.2. Appoint an OPSEC monitor and identify them to the 16 SOW program manager.

A4.1.1.3. Integrate the OPSEC concept into their mission plans and activities.

A4.1.1.4. Ensure every person under their command understands the OPSEC concept as the way in which we conduct Air Force business; the mission Critical information they need to know; the job related OPSEC indicators of that information; and the OPSEC measures employed or contemplated to neutralize any OPSEC vulnerabilities.

A4.1.1.5. Ensure OPSEC measures are appropriately developed and executed to reinforce the combat effectiveness of units, defense systems and weapon systems.

A4.1.1.6. Centrally manage OPSEC guidance concerning Critical information to ensure consistency throughout each organization and across organizational lines.

A4.1.1.7. Be the decision-maker for risk acceptance when no countermeasures are acceptable.

A4.2. All Personnel will:

A4.2.1. Attend annual OPSEC training

A4.2.2. Practice good OPSEC

A4.2.3. Ensure OPSEC countermeasures are included when passing sensitive information

A4.2.4. Use OPSEC POCs

A4.2.5. Discuss OPSEC concerns with family members

A4.3. PROGRAM MANAGER RESPONSEBILITIES

A4.3.1. HQ AFSOC OPSEC Program Manager will:

A4.3.1.1. Establish a command OPSEC program IAW AFSOCI 10-101

A4.3.1.2. Establish and maintain command critical information list

A4.3.1.3. Maintain liaison with other agencies, activities, and command for the purposes of coordination, training, information, and operational support

A4.3.1.4. Represent AFSOC at OPSEC conferences and meetings

A4.3.1.5. Assist accomplishment of surveys and assessments

A4.3.1.6. Coordinate program operations and activities with USSOCOM as may be necessary to provide assistance and technical support for the AFSOC staff and subordinate units

A4.3.1.7. Develop and maintain the command OPSEC training program

A4.3.1.8. Produce and distribute to B-Staff and Unit program managers a self- inspection checklist

A4.3.1.9. Maintain AFSOCI 10-1101. Provide copy to USSOCOM and HQ USAF

A4.3.1.10. Coordinate non-intelligence interagency support through USSOCOM

A4.3.1.11. Manage command survey program

A4.3.1.12. Prioritize OPSEC initiatives, surveys, and counter measure implementation

A4.3.1.13. Host semi-annual Command OPSEC Meeting

A4.3.1.14. Maintain OPSEC database

A4.3.1.15. Review sub-unit program goals and objectives for consistency

A4.3.1.16. Submit annual report to USSOCOM

A4.3.1.17. Maintain OPSEC library:

A4.3.1.17.1. Publications

A4.3.1.17.2. Training material and video tapes

A4.3.1.17.3. After action reports

A4.3.1.18. Inform supported organization of AFSOC/CC decision to risk exploitation

A4.3.2. 16 SOW OPSEC Program Managers and HHQ Program Managers POCs will:

A4.3.2.1. Receive advanced OPSEC training to conduct surveys and planning

A4.3.2.2. Coordinate OPSEC with supporting and contractor organizations

A4.3.2.3. Facilitate the acceptance and implementation of OPSEC throughout their organization

A4.3.2.4. Integrate the OPSEC concept into organizational plans and activities

A4.3.2.5. Advise commanders and other primary decision-makers on OPSEC matters

A4.3.2.6. Coordinate on (and facilitating the development of) OPSEC plans and measures for operations, activities, and exercises

A4.3.2.7. Integrate OPSEC requirements into C2W and information warfare strategies

A4.3.2.8. Develop, maintain and market the organization’s OPSEC program

A4.3.2.9. Ensure all personnel receive appropriate OPSEC training

A4.3.2.10. Provide OPSEC program requirements for intelligence and Counter Intelligence support

A4.3.2.11. Coordinate OPSEC requirements with public affairs officers

A4.3.2.12. Assist in determining guidelines for controlling mission critical information and sensitive activities

A4.3.2.13. Coordinate and facilitate OPSEC surveys

A4.3.2.14. Maintain an effective rapport with Foreign Intelligence and counter intelligence agencies

A4.3.2.15. Participate in OPSEC process that relate to unit/division

A4.3.2.16. Provide HHQ program manager with information to update OPSEC databases

A4.3.2.17. Participate in the Semi-annual Command OPSEC Meetings

A4.3.2.18. Report deficiencies improvement opportunities at Semi-annual meetings

A4.3.2.19. Nominate activities for OPSEC surveys

A4.3.2.20. Annually accomplish the self-inspection checklist

A4.3.2.21. Maintain continuity folder

A4.3.3. Unit OPSEC Program Managers (in addition to A4.2.) will :

A4.3.3.1. Establish an OPSEC program IAW HFI 10- 1101

A4.3.3.2. Include OPSEC awareness in newcomer and spouse orientations

A4.3.3.3. Prioritize OPSEC initiatives, surveys, and CM implementation

A4.3.3.4. Conduct annual OPSEC appraisals

A4.3.3.5. Submit annual report

A4.3.3.6. Maintain OPSEC library:

A4.3.3.6.1. Publications

A4.3.3.6.2. Training material and video tapes

A4.3.3.6.3. After action reports

A4.3.3.6.4. Include OPSEC considerations in evaluations of training tests, readiness inspections, and field exercises

A4.4. USAFSOS OPSEC Program Manager (in addition to A4.2. and A4.3.) will:

A4.4.1. Evaluate courses for appropriateness of OPSEC instruction

A4.4.2. Include OPSEC in formal education and training as appropriate

A4.5. 18 FLTS will:

A4.5.1. Develop standing critical information List (with indicators) and CMs for tactics development and test and evaluation

A4.5.2. Participate in vulnerability analyses for test and evaluation of AFSOC systems

Attachment 5

16 SOW STANDING CRITICAL INFORMATION LIST (CIL) – WITH SOME EXAMPLES OF COMMON INDICATORS

A5.1. Concept of Operations, planned activities

A5.1.1. Exercise CONOPS, SOPs

A5.1.2. Deconfliction coordination, schedules

A5.2. Rehearsals; Association with PLAN, results

A5.2.1. Unscheduled or dramatically changed exercise

A5.2.2. Rapid changes of procedures

A5.3. Deception Plans

A5.3.1. Uncorroborated information leaks

A5.4. PSYOPS Plans

A5.4.1. Coordination with PSYOPS Units

A5.5. Trigger events for execution

A5.5.1. Speculation by associated but unofficial personnel

A5.6. Timing for Deployment, Execution, Redeployment

A5.6.1. Support activities

A5.7. Locations of Operations

A5.7.1. Site surveys, request for information

A5.8. C3 Architecture

A5.8.1. SOPs, increased COMM traffic with a unit/HHQ, COMMEXs

A5.8.2. Urgent requests for communication devices

A5.9. Open source reporting

A5.10. Participating Organizations

A5.10.1. Telephone calls between units, deployed phone list

A5.11. Key Personnel; Locations, Itineraries

A5.11.1. Schedules, protocol coordination

A5.12. Vulnerabilities, Shortfalls, Limitations, Restrictions

A5.12.1. SITREPs, Mission Needs Statements, FCIF and MAPs and Weapon System Roadmap

A5.13. New or improved Tactics or Capabilities

A5.14. Rules of Engagement

A5.14.1. Issue of specialized ammunition/weapons

A5.15. Logistics; Nodes, Supply Lines

A5.15.1. Coordination with suppliers or users

A5.16. Friendly and Threat Intelligence Capabilities, Operations

A5.16.1. Friendly and Threat Intelligence Capabilities, Operations

A5.17. Effectiveness of Threat Actions

A5.17.1. Instructions to change standard procedures

NOTE:

This list is NOT all-inclusive. It is provided as a starting point only. When presented with a specific operation you should use the most specific information available to produce a tailored CIL.

Attachment 6

16 SOW OPSEC TRAINING REQUIREMENTS

A6.1. OPSEC Training must include the following topics:

A6.1.1. Introduction to OPSEC

A6.1.1.1. What is OPSEC

A6.1.1.2. How does it differ from and relate to traditional security areas?

A6.1.1.3. How does it benefit us?

A6.1.1.4. Examples, positive and negative

A6.1.2. OPSEC program structure

A6.1.2.1. Unit OPSEC POCs*

A6.1.2.2. HHQ OPSEC POCs

A6.1.2.3. AFSOC OPSEC POCs

A6.1.2.4. USSOCOM OPSEC POCs

A6.1.2.5. USAF OPSEC POCs

A6.1.2.6. Supporting unit POCs*

A6.1.2.7. Supported unit POCs*

A6.1.3. Five step OPSEC process

A6.1.3.1. Identifying Critical information and Indicators

A6.1.3.2. Threat Assessment

A6.1.3.3. Vulnerability Analysis

A6.1.3.4. Risk Assessment

A6.1.3.5. Determining and Implementing Countermeasures (CMs)

A6.1.4. Tools/sources of information

A6.1.4.1. Regulations

A6.1.4.2. Publications

A6.1.4.3. Plans/Roadmaps

A6.1.4.4. Databases

A6.1.4.5. Formal schools/training available

A6.1.5. Standing critical information, Indicators, and CMs

A6.1.5.1. Command

A6.1.5.2. Unit*

A6.1.5.3. Other associated organizations*

A6.1.6. How does the individual fit into the OPSEC process?

A6.1.6.1. Individual responsibilities/duties

A6.1.6.2. Responsibilities/tasks of individuals office*

* Information not in 16 SOW training material. Developing and presenting this information is the responsibility of the unit/directorate OPSEC office.

Attachment 7

16 SOW OPSEC SELF-INSPECTION CHECKLIST

A7.1. Is the commander's involvement in and support of the unit OPSEC program evident? Has the commander issued an OPSEC implementing document?

A7.2. Has an OPSEC Officer and/or NCO from all agencies specified in HFI 10-1101 been appointed, in writing, to act as the focal point for all OPSEC matters?

A7.3. Has the unit OPSEC Monitor attended an OPSEC practitioner's course or program manager's course? If no, has one been scheduled through the 16 SOW Program Manager?

A7.4. Are the unit's OPSEC monitors knowledgeable about OPSEC concepts, procedures and objectives?

A7.5. Are unit personnel aware of the identities of the unit OPSEC monitors?

A7.6. Have the names of the OPSEC monitors been forwarded to the 16 SOW Program Manager?

A7.7. Does the local OPSEC program ensure the active participation and involvement of the entire staff or unit?

A7.8. Does the unit have an effective OPSEC training program? Does the unit update its Critical information annually?

A7.9. Is the unit complying with annual OPSEC training requirements identified in HFI 10-1101? Are all personnel receiving training? Is it documented?

A7.10. Does the unit develop its own training information, such as critical information, indicators, countermeasures, unit responsibilities, and reminders?

A7.11. Are personnel aware of the OPSEC threat from various intelligence collection methods?

A7.12. Do unit personnel clearly understand the interrelationship of COMSEC, OPSEC, physical security, and information security?

A7.13. Does the unit have HFI 10-1101 or other applicable directives, which define unit OPSEC program requirements, responsibilities, and procedures?

A7.14. Does each PLAN or OPORD contain a complete Annex L, to include a list of critical information, prior to publication to ensure OPSEC guidelines have been followed?

A7.15. Are all members aware of OPSEC considerations/responsibilities as related to the planning process? Is the OPSEC process started at the very beginning of planning?

A7.16. Is OPSEC a graded item on all formal unit inspections?

A7.17. Are published OPSEC surveys and after action reports/trip reports reviewed for possible application of findings or “lessons learned” to local on going or planned activities?

A7.18. Has the need for an OPSEC survey been determined? If so, has one been conducted? If not, has one been scheduled or requested?

A7.19. Have actions been taken on recommendations to correct weakness or deficiencies noted in the OPSEC survey?

A7.20. Do unit OPSEC monitors participate in semi-annual OPSEC meetings?

A7.21. Do they report deficiencies/improvement opportunities at semi-annual meetings?

A7.22. Do unit OPSEC monitors nominate activities for OPSEC surveys at these meetings?

A7.23. Is this information from the semi-annual meetings passed on to unit personnel and subordinate units/flights?

A7.24. Does the 16 SOW program manager publish an annual report IAW HFI 10-1101?

Attachment 8

FLOW DESCRIPTION FOR TRAINING EXERCISES

A8.1. Exercise proposal/directive to 16 SOW. OPSEC for exercise must address both scenario and real-world critical information.

A8.1.1. Is exercising OPSEC process an objective?

A8.1.2. No: Continue with this flow description to protect real-world critical information that could be revealed by the exercise.

A8.1.3. Yes: OPR/16 OG DOX use flow description for contingency operations during exercise planning conference in addition to continuing with this flow description.

A8.1.4. Is exercise HHQ directed?

A8.1.5. No: 16 SOW/XPE determine OPR/level for OPSEC coordination (16 SOW ,Group, Squadron). OPR will develop initial CIL.

A8.1.6. Yes: Is CRITICAL INFORMATION LIST (CIL) included?

A8.1.7. No: 16 SOWXPE request CIL from supported organizations.

A8.1.8. Supported organization responds with CIL?

A8.1.9. No: Request CIL through OPSEC POC chain: (SQ, GP, WING, AFSOC).

A8.1.10. Yes: Use

A8.2. OPR/XPE search OPSEC database/JULLS for similar exercises

A8.2.1. Search positive?

A8.2.2. No: Use supported organization's CIL and/or CIL from OPLAN/CONPLAN/EXPLAN being exercised plus 16 SOW HFI 10-1101 CIL as basis for initial CIL. Component Manual is a useful tool to determine CIL. Contact 16 SOW/CV for command input.

A8.2.3. Yes: Use with CIL from supported OPLAN/EXPLAN/organization to develop initial CIL.

A8.3. OPR/XPE Provide initial CIL to functional area and subordinate unit planners to develop their CIL. Critical information Component Manual is a useful tool to determine CIL. List of CIL with associated indicators returned to OPR/DOX for compilation.

A8.4. OPR/XPE Provides compiled 16 SOW CIL with indicators to OSI and OPR/IN for detailed and specific THREAT ASSESSMENT (what does he already know and how does he know it?). Assessment provided to OPR/DOX.

A8.5. OPR and subordinate unit OPSEC monitors conduct VULNERABILITY ANALYSIS with functional area planners.

A8.5.1. Survey required (no information in OPSEC database, new PLAN being exercised, change of threat, tactics, participants)?

A8.5.2. No: Conduct assessment (minimum participants DOX/IN/LG/SC)

A8.5.3. Yes: Conduct survey IAW Joint Pub 3-54 Appendix E and JCS OPSEC Survey Guide, or National Cryptological School Guide to performing OPSEC assessments.

A8.5.4. Evaluate each CIL item and associated indicators

A8.5.5. Does threat have capacity to acquire CIL information? Is he in place to acquire it? Does he have the indicators to begin collection on it?

A8.5.6. No to any: Move to next item

A8.5.7. Yes to any: Identify for risk assessment

A8.6. OPR conducts risk assessment with functional areas and subordinate unit planners. Close coordination with supporting and supported unit planners recommended during this step.

A8.6.1. Risk Assessment Process

A8.6.1.1. Prioritize risks

A8.6.1.2. Determine possible countermeasures for each risk

A8.6.1.3. Assess each countermeasure (CM)

A8.6.1.4. Does vulnerability justify CM cost?

A8.6.2. No: Drop from list. If CM is questionable or not acceptable to16 SOW/CC, pass through OPSEC program chain. The decision to risk exploitation by threat. Inform supported organization of risk.

A8.6.3. Yes: Determine if it is the best CM

A8.7. OPR Disseminate selected CMs to exercise participants.

A8.8. OPSEC Critical information and countermeasures will be briefed to participants and affected supporting organizations by their respective OPSEC officers and will be included in the mass exercise/deployment briefing. OPR should ensure the information is also included in exercise directive and aircrew flimsy. Both exercise scenario and real world OPSEC will be briefed and clearly identified as one or the other.

A8.9. Review and update OPSEC plan as the situation changes.

Attachment 9

FLOW DESCRIPTION FOR CURRENT OPERATIONS TO INCLUDE SORTS AND DEPLOYMENT REPORTING

A9.1. 16 SOW or unit directed operations?

A9.1.1. No: 16 OG/DOO request CIL (if any) and countermeasures (CMs) from supported unit. Use as appropriate in conjunction with 16 SOWCIL and CMs.

A9.1.2. Yes: Go to step **A9.2.**

A9.2. Unit/DOO search 16 SOW database for similar OPS

A9.2.1. Search positive?

A9.2.2. No: Accomplish full five step OPSEC process

A9.2.3. Yes: Adhere to the identified Critical Information List (CIL) and CMs. Go to step **A9.7.**

A9.3. Unit/DOO provide initial CIL (from HFI 10-1101 and supported unit inputs) to functional area and subordinate unit planners to develop their CIL. Critical information Component Manual is a useful tool to determine CIL. List of CIL with associated indicators returned to unit/DOO.

A9.4. Unit/DOO provides compiled 16 SOW CIL with indicators to OSI and Unit/IN for detailed and specific threat assessment (what does he already know and how does he know it?). Assessment provided to Unit /DOO.

A9.5. Unit/DOO and subordinate unit OPSEC monitors conduct vulnerability analysis with functional area planners.

A9.5.1. Survey required (no information in OPSEC database, threat significant)?

A9.5.2. No: Conduct assessment (minimum participants DO/IN/LG/SC)

A9.5.3. Yes: Conduct survey IAW Joint Pub 3-54 Appendix E and JCS OPSEC Survey Guide, or National Cryptological School Guide to performing OPSEC Assessments.

A9.5.4. Evaluate each CIL item and associated indicators

A9.5.5. Does threat have capacity to acquire CIL information? Is he in place to acquire it?

A9.5.6. Does he have the indicators to begin collection on it?

A9.5.7. No to any: Move to next item

A9.5.8. Yes to any: Identify for risk assessment

A9.6. Unit/DOO conducts RISK ASSESSMENT with functional areas and subordinate unit planners. Close coordination with supporting and supported unit planners recommended during this step.

A9.6.1. Risk Assessment Process

A9.6.1.1. Prioritize risks

A9.6.1.2. Determine possible countermeasures for each risk

A9.6.1.3. Assess each countermeasure (CM)

A9.6.1.4. Does vulnerability justify CM cost?

A9.6.2. No: Drop from list. If CM is questionable or not acceptable to 16 SOW/CC, pass through OPSEC program chain. The decision to risk exploitation by threat. Inform supported organization of risk.

A9.6.3. Yes: Determine if it is the best CM.

A9.7. Unit/DOO disseminates selected CMs to exercise participants.

A9.8. Unit/DOO documents OPSEC plan in 16 SOW database. OPSEC CMs for routine and recurring operations and reports will be coordinated with the Wing's program manager, at the semi-annual OPSEC meeting, for inclusion in the annual OPSEC training program.

A9.9. Review and update OPSEC plan as the situation changes.

NOTE:

This flow description will deal only with routine operations and reporting. As these are recurring operations, the full five step OPSEC process need only to be accomplished once, then updated as required by changes.

Attachment 10

FLOW DESCRIPTION FOR CONTINGENCY OPERATIONS

A10.1. HHQ Tasking to 16 SOW

A10.1.1. Critical Information List (CIL) included?

A10.1.2. No: Request CIL from OPSEC POC chain.

A10.1.3. Tasker responds with CIL?

A10.1.4. No: Request CIL through OPSEC POC chain.

A10.1.5. Yes: Use

A10.1.6. Yes: 16 SOW /DOX use as basis for own CIL

A10.2. 16 OG/DOX search OPSEC database/JULLS for similar exercises

A10.2.1. Search positive?

A10.2.2. No: Use supported organization's CIL and/or CIL from OPLAN/CONPLAN plus 16 SOW HFI 10-1101 CIL as basis for initial CIL. Component Manual is a useful tool to determine CIL. Contact 16 SOW/CV for command input.

A10.2.3. Yes: Use with CIL from supported organization to develop initial CIL.

A10.3. 16 SOW/XPD provide initial CIL to functional area and subordinate unit planners to develop their CIL. List of CIL with associated indicators returned to 16 SOW/DOX for compilation.

A10.4. 16 SOW/XPD provides compiled 16 SOW CIL with indicators to OSI and OPR/IN for detailed and specific threat assessment (what does he already know and how does he know it?). Assessment provided to OPR/DOX.

A10.5. 16 SOW/XPD and subordinate unit OPSEC monitors conduct vulnerability analysis with functional area planners.

A10.5.1. Survey required (no information in OPSEC database, new; threat, tactics, participants) and time available?

A10.5.2. No: Conduct Assessment (minimum participants DOX/IN/LG/SC)

A10.5.3. Yes: Conduct survey IAW Joint Pub 3-54 Appendix E and JCS OPSEC Survey Guide, or National Cryptological School Guide to performing OPSEC Assessments.

A10.5.4. Evaluate each CIL item and associated indicators

A10.5.5. Does threat have capacity to Acquire CIL information? Is he in place to acquire it? Does he have the indicators to begin collection on it?

A10.5.6. No to any: Move to next item

A10.5.7. Yes to all: Identify for risk assessment IAW **A10.6.** 16 OG/DOX conducts risk assessment with functional areas and subordinate unit planners. Close coordination with supporting and supported unit planners recommended during this step.

A10.5.7.1. Risk Assessment Process

A10.5.7.1.1. Prioritize risks

A10.5.7.1.2. Determine possible countermeasures for each risk

A10.5.7.1.3. Assess each countermeasure (CM)

A10.5.7.1.4. Does vulnerability justify CM cost?

A10.5.7.2. No: Drop from list. If CM is questionable or not acceptable to 16 SOW /CC, through OPSEC program chain, for decision to risk exploitation by threat. Inform supported organization of risk.

A10.6. 16 OG/DOX disseminates selected CMs to exercise participants.

A10.7. 16 OG/DOX documents OPSEC plan in ANNEX L of the 16 SOWEXPLAN or OPROD. Subordinate units include OPSEC plan in their supporting plan or FRAGORD.

A10.8. Review and update OPSEC plan as the situation changes.